The Ethics of Cloud Computing

Ethical Challenges on the Horizon: Confidentiality, Competence and Cloud Computing

Catherine Sanders Reach
Chicago Bar Association
Chicago, IL

Rachel Packer
Zucker, Goldberg & Ackerman, LLC.
Mountainside, NJ

Paul Bateman
Schiff Hardin LLP
Chicago, IL

Reprinted with Permission
Ethical Challenges on the Horizon:
Confidentiality, Competence and Cloud Computing

John M. Barkett
Shook, Hardy & Bacon L.L.P.
Miami, Florida

Table of Contents

Introduction ...........................................................................................................................................3
Model Rules Relied Upon in Cloud Computing Ethics Opinions .....................................................3
  Competence Under Model Rule 1.1 ...................................................................................................3
  Model Rule 1.6 and the Duty of Confidentiality ............................................................................4
  Model Rules 1.15 and 1.16 and Safeguarding Property .................................................................5
  Model Rules 5.1 and 5.2 and the Responsibilities of Partners and Subordinate Lawyers ...............5
  Model Rule 5.3 and Responsibilities Regarding Nonlawyer Assistants ......................................7
  Model Rule 1.4 and Communications with Clients .......................................................................8
ABA Commission on Ethics 20/20 and Recent Changes to the Model Rules .................................9
  Model Rule Changes: Technology and Confidentiality .........................................................10
  Model Rule Changes: Outsourcing .........................................................................................11
State Bar Ethics Opinions On Cloud Computing/Storage .................................................................13
  Oregon Bar Ethics Opinion 2011-188 (November 2011) .........................................................13
  Pennsylvania Formal Opinion 2011-200 .................................................................................15
  New York State Bar Ethics Opinion 842 (Sept. 10, 2010) .......................................................21
  Alabama Ethics Opinion 2010-02 ............................................................................................21
  Washington State Bar Advisory Opinion 2215 (2012) ............................................................22
  Iowa Bar Ethic Opinion 11-01 (September 9, 2011) .................................................................23
  Vermont Ethics Opinion 2010-6 ...............................................................................................24
  Massachusetts Bar Ethics Opinion 12-03 (May 17, 2012) ........................................................26
  New Hampshire Ethics Committee Advisory Opinion #2012-13/4 .........................................27
  Florida Bar Proposed Advisory Opinion 12-3 (January 25, 2013) .........................................30
State Bar Ethics Opinions on Remote Storage of Electronic Data ..................................................30
  California State Bar Standing Committee on Professional Responsibility and Conduct Formal
  Opinion 2010-179 ....................................................................................................................30
INTRODUCTION

Anyone who uses a social media Web site or who has uploaded photographs to a photo-sharing site is engaged in “cloud computing.” A computer user also “lives in the cloud” when using software as a service (SaaS) instead of buying software for installation on an office computer, and then storing documents on a cloud server—Microsoft Office 365, Dropbox, Google Docs—so that they can be accessed anytime from anywhere as long as the individual has an Internet connection.

Lawyers have among the largest repositories of documents of any profession. Storage is an expense to a law firm. Cloud storage is relatively cheap. It is also convenient because it gives lawyers and their clients access to the documents from anywhere, again, as long as there is an Internet connection.

When they store client documents, lawyers are also fiduciaries. Model Rule 1.15 is entitled “Safekeeping Property” and requires lawyers to do just that in ways that are “appropriate.” Is cloud storage “appropriate”? The short answer based on several state bar ethics opinions is, “yes”: storage of electronic client documents in a third-party electronic-storage medium accessed over the Internet can be an ethically acceptable law firm filing cabinet. Why do I emphasize “can be”? Because these ethics opinions set forth ethical parameters for storage of documents in a cloud environment that may be too daunting for lawyers concerned about the risk of a breach of data security.

After first identifying ethics rules that are typically invoked by state bar ethics committees in this cyber arena, I then discuss a number of ethics opinions on the use of cloud computing and electronic storage of confidential client information.

MODEL RULES RELIED UPON IN CLOUD COMPUTING ETHICS OPINIONS

Ethics opinions that discuss cloud computing focus on the same ethics rules.

Competence Under Model Rule 1.1

Model Rule 1.1 provides:
A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Comment [1] to Model Rule 1.1 identifies relevant factors in determining whether a lawyer has the requisite knowledge and skill to handle a particular matter. They include,

the relative complexity and specialized nature of the matter, the lawyer’s general experience, the lawyer’s training and experience in the field in question, the preparation and study the lawyer is able to give the matter and whether it is feasible to refer the matter to, or associate or consult with, a lawyer of established competence in the field in question.¹

Model Rule 1.6 and the Duty of Confidentiality

Lawyers have a duty to protect the confidences of their clients. Model Rule 1.6 contains the basic “confidentiality” obligations of lawyers. Rule 1.6(a) provides that a lawyer “shall not” reveal information “relating to representation of a client unless the client gives informed consent,”² the disclosure is “impliedly authorized in order to carry out the representation,”³ or the disclosure is permitted by Rule 1.6(b).⁴

Comment [16] of Model Rule 1.6 succinctly provides:

A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision. See Rules 1.1, 5.1 and 5.3.⁵

¹ Comment [5] to Model Rule 1.1 adds that handling a matter competently “includes inquiry into and analysis of the factual and legal elements of the problem, and use of methods and procedures meeting the standards of competent practitioners. It also includes adequate preparation. The required attention and preparation are determined in part by what is at stake; major litigation and complex transactions ordinarily require more extensive treatment than matters of lesser complexity and consequence. An agreement between the lawyer and the client regarding the scope of the representation may limit the matters for which the lawyer is responsible. See Rule 1.2(c).” Rule 1.2(c) provides: “A lawyer may limit the scope of the representation if the limitation is reasonable under the circumstances and the client gives informed consent.” Attending appropriate training programs may also be necessary.

² Informed consent “denotes the agreement by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct.” Model Rule 1.0(e).

³ To illustrate this second exception, comment [5] to Rule 1.6 explains that a lawyer is impliedly authorized to admit a fact that cannot be disputed or to make a disclosure that facilitates a satisfactory conclusion to a matter. Lawyers in a firm may also disclose information to each other relating to a client in the firm “unless the client has instructed that particular information be confined to particular lawyers.”

⁴ Rule 1.6(b) is not applicable in this context.

⁵ Model Rules 5.1 and 5.3 are discussed below.
Model Rules 1.15 and 1.16 and Safeguarding Property

As noted in the Introduction, Model Rule 1.15(a) creates a fiduciary obligation on lawyers to safeguard client property, which includes client documents. It provides:

A lawyer shall hold property of clients or third persons that is in a lawyer’s possession in connection with a representation separate from the lawyer’s own property. Funds shall be kept in a separate account maintained in the state where the lawyer’s office is situated, or elsewhere with the consent of the client or third person. Other property shall be identified as such and appropriately safeguarded. Complete records of such account funds and other property shall be kept by the lawyer and shall be preserved for a period of [five years] after termination of the representation.

What are appropriate safeguards for confidential documents stored in a cloud environment? As explained in the ethics opinions discussed below, this is not an easily answered question for client-confidential documents.

Model Rule 1.16(d) addresses termination but also discusses handling of client documents. It provides:

Upon termination of representation, a lawyer shall take steps to the extent reasonably practicable to protect a client’s interests, such as giving reasonable notice to the client, allowing time for employment of other counsel, surrendering papers and property to which the client is entitled and refunding any advance payment of fee or expense that has not been earned or incurred. The lawyer may retain papers relating to the client to the extent permitted by other law.

If a lawyer is managing litigation support for a client that includes the management of electronically stored information, the lawyer and the client should have a suitable arrangement for the storage, protection, and return of the electronically stored information.

Model Rules 5.1 and 5.2 and the Responsibilities of Partners and Subordinate Lawyers

Model Rule 5.1 provides:

(a) A partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.

(b) A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.

(c) A lawyer shall be responsible for another lawyer’s violation of the Rules of Professional Conduct if:
(1) the lawyer orders or, with knowledge of the specific conduct, ratifies the conduct involved; or

(2) the lawyer is a partner or has comparable managerial authority in the law firm in which the other lawyer practices, or has direct supervisory authority over the other lawyer, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

Model Rule 5.2 provides in full:

(a) A lawyer is bound by the Rules of Professional Conduct notwithstanding that the lawyer acted at the direction of another person.

(b) A subordinate lawyer does not violate the Rules of Professional Conduct if that lawyer acts in accordance with a supervisory lawyer’s reasonable resolution of an arguable question of professional duty.

The message of these rules is not complicated. Lawyers must reasonably ensure that those whom they oversee are competent under Model Rule 1.1 and are otherwise in compliance with the applicable rules of professional conduct (RPC).

Similarly, lawyers who are overseen by others are still bound by the RPC even if they are taking direction from another lawyer. The subordinate lawyer must speak up if the RPC are not being followed by the supervisory lawyer.

Under Model Rule 5.1, there is an “actual knowledge” requirement to hold a supervisory lawyer responsible for the failure of a supervised lawyer to comply with the RPC. However, lawyers must be aware of differences between Model Rule 5.1 and the rule as it has been adopted in a particular jurisdiction. Illustratively, the District of Columbia has a “knew or should have known” requirement. D.C. Rule 5.1(c)(2) provides in pertinent part that a lawyer “shall be responsible for another lawyer’s violation of the Rules of Professional Conduct if”:

The lawyer has direct supervisory authority over the other lawyer or is a partner or has comparable managerial authority in the law firm or government agency in which the other lawyer practices, and knows or reasonably should know of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

In Re Cohen, 847 A.2d 1162 (D.C. 2004) illustrates the importance of this difference. An associate in a law firm withdrew a trademark application for a client, Dr. Schleicher, telling the Patent and Trademark Office that the client had “expressly abandoned its above-referenced trademark application.” Id. at 1166. The statement was false. The client was not aware of the filing and had not endorsed it. The PTO accepted the abandonment of the application. The associate was supervised by Cohen. Disciplinary proceedings were instituted against Cohen. The D.C. Board of Professional Responsibility found Cohen to be in violation of, among others, D.C. Rule 5.1(c)(2). Cohen conceded that “there was no system in place to impart rudimentary ethics training to lawyers in the firm,” and
there was no “review mechanism which allowed an associate’s work to be reviewed and guided by a supervisory attorney.” But he argued that he should not be punished for professional misconduct where he had no actual knowledge of the associate’s misrepresentation. *Id.* The D.C. Court of Appeals rejected the plea.

*Rule 5.1(c)(2) in this jurisdiction represents a judgment that attorneys supervising other lawyers must take reasonable steps to become knowledgeable about the actions of those attorneys in representing clients of the firm. As the Board explained, the “reasonably know” provision was carefully crafted to encourage — indeed to require — supervising attorneys to reasonably monitor the course of a representation such as respondent’s firm had undertaken on behalf of Dr. Schleicher, denying them the ostrich-like excuse of saying, in effect, “I didn’t know and didn’t want to know.”*

...  

In reaching this conclusion, the Board took into account a number of factors including the discreet nature of the case, the extended length of the representation, the small size of the firm, and of course, the degree of supervision or lack thereof. The Board stated:

“*Therefore, in the particular circumstances of this case, we conclude that Bar Counsel has established a violation of Rule 5.1(c)(2) because respondent reasonably should have known of the withdrawal application and should have been able to take reasonable remedial action to avoid its consequences. We believe a lawyer of reasonable prudence and competence would have made the inquiry necessary to determine the status of the application proceeding.”*

*We adopt this conclusion given the circumstances of this case.*

*Id.* at 1166-67. This case illustrates the importance to supervisory lawyers not only of knowing your jurisdiction’s counterpart to Model Rule 5.1, but also what supervised lawyers are doing. Hence, decisions about the use of cloud-computing services delegated to the more computer savvy lawyers in a law firm still can have professional conduct consequences for lawyers in a supervisory position.

**Model Rule 5.3 and Responsibilities Regarding Nonlawyer Assistants**

Model Rule 5.3 provides:

*With respect to a nonlawyer employed or retained by or associated with a lawyer:*

(a) a partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person’s conduct is compatible with the professional obligations of the lawyer;
(b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person’s conduct is compatible with the professional obligations of the lawyer; and

(c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:

(1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or

(2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

The use of an outside vendor to store client information electronically would be governed by this provision.6

Model Rule 1.4 and Communications with Clients
Model Rule 1.4 is entitled “Communication” and contains these requirements:

(a) A lawyer shall:

(1) promptly inform the client of any decision or circumstance with respect to which the client’s informed consent, as defined in Rule 1.0(e), is required by these Rules;

(2) reasonably consult with the client about the means by which the client’s objectives are to be accomplished;

(3) keep the client reasonably informed about the status of the matter;

(4) promptly comply with reasonable requests for information; and

(5) consult with the client about any relevant limitation on the lawyer’s conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law.

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

---

6 While lawyers have an ethical obligation to supervise vendors, they also face a sanctions risk in litigation if their vendors err. See In Re Seroquel Products Liability Litigation, 2007 U.S. Dist. LEXIS 61287, *49-50 (M.D. Fla. Aug. 21, 2007) (a party is responsible for the errors of its vendors, citing Sedona Principle 6.d: “Ultimate responsibility for ensuring the preservation, collection, processing, and production of electronically stored information rests with the party and its counsel, not with the nonparty consultant or vendor.”).
A lawyer proposing to store confidential information in a cloud environment will have to account for these requirements in evaluating cloud storage vendors, service agreements, and service reliability, all among the topics which are the subject of Model Rule amendments and state bar ethics committees opinions that have entered the world of cloud storage.

ABA COMMISSION ON ETHICS 20/20 AND RECENT CHANGES TO THE MODEL RULES

The ABA Commission on Ethics 20/20 was formed to consider changes to the Model Rules of Professional Conduct with an eye in part on the intersection of lawyers’ conduct and advances in technology. Its Working Group on the Implications of New Technologies published an “Issues Paper Concerning Confidentiality and Lawyers’ use of Technology” (September 20, 2010). The Working Group identified a number of confidentiality problems with “cloud computing” that will establish a good framework for putting into context the ethics opinions discussed below. The confidentiality problems identified in the Working Group’s Issues Paper are:

- Unauthorized access to client-confidential data by a vendor’s employees, subcontractors, or third parties (e.g., hackers) and protection against the acts of disgruntled or dishonest employees or subcontractors with access to client data;
- Storage of client data in countries with fewer legal protections for electronically stored information than would exist in the United States or countries with protections similar to those in the United States;
- The adequacy of back-up processes by the cloud storage vendor and processes to restore data if (a) there is a technical failure, a server crashes, (b) data becomes corrupted or destroyed inadvertently or due to an accident, natural disaster or terrorist attack, or (c) a virus or other malware infects the data;
- Unclear policies regarding data ownership;
- Maintaining access to stored data if the cloud-computing vendor (a) is terminated, (b) leaves the business, (c) goes out of business or files for bankruptcy, or (d) suffers from a temporary business interruption;
- Unclear policies addressing notice in the event of a breach of the data security systems;
- Insufficient encryption of the client’s data;
- Procedures for responding to government requests for information, or access to information, including procedures for resisting such requests where that might be appropriate;
- Policies to address destruction of data when the lawyer no longer wants the data or when a client changes lawyers, and procedures to transfer data if a client seeks to change the vendor;

---

7 See http://www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html.
• When and to what extent a client’s consent is required before using cloud-computing vendor services; and
• The format of stored data and its compatibility with software platforms other than that of the cloud computer provider.

The Commission also invited “comments on whether lawyers have an obligation to negotiate particular terms and conditions before incorporating cloud-computing services into their law practices” and, if so, “what the terms and conditions should state and what the Commission’s recommendations in this area should be.”

Model Rule Changes: Technology and Confidentiality

Since the Issue Paper was promulgated, the Commission adopted a resolution on “technology and confidentiality” that was approved by the ABA House of Delegates in August 2012. The approval resulted in five changes to the Model Rules. Two of these changes would relate to cloud-computing services. I summarize both changes here:

1. Comment [6] to Rule 1.1 addressing competence now includes the following highlighted clause:

   “[6] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.” This provision will require lawyers to better understand any advances in technology that genuinely relate to competent performance of the lawyer’s duties to a client.

2. Model Rule 1.6, addressing confidentiality of information, has been amended by this addition:

   “(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.” This change is accompanied by new text in Comment [16]. This additional text is directly related to use by a lawyer of a cloud storage vendor:

   The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer’s efforts include, but are not limited to, the sensitivity of the information, the

---

9 Because cloud computing is a form of outsourcing, the Commission referenced ABA Formal Opinion 08-451 that addressed the ethics of outsourcing legal or nonlegal support services.


ABA Ethics Op. 08-451 requires lawyers who wish to demonstrate compliance with their competency obligation in Model Rule 1.1 to properly supervise the provider of the outsourcing services as required under Model Rules 5.1 and 5.3; make appropriate disclosures to the client; obtain client consent if the outsourcing service provider is going to receive information protected by Model Rule 1.6; charge a reasonable fee under and otherwise comply with Model Rule 1.5; and avoid assisting in the unauthorized practice of law in compliance with Model Rule 5.5. For a discussion of ethics opinions on outsourcing, see John M. Barkett, The Ethics of E-Discovery (Chicago: First Chicago Press, 2009), 81-97.
likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client’s information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer’s duties when sharing information with nonlawyers outside the lawyer’s own firm, see Rule 5.3, Comments [3]-[4].

Model Rule Changes: Outsourcing

The Commission adopted another resolution that was approved by the ABA House of Delegates to amend the Model Rules with respect to outsourcing.¹⁰

The title to Model Rule 5.3 has been slightly modified to change the word “Assistant” to “Assistance” so that it now reads: “Rule 5.3 Responsibilities Regarding Nonlawyer Assistance.” New Comment [3] provides that a lawyer may use nonlawyers outside of the law firm to assist the lawyer and gives as one example, “using an Internet-based service to store client information.”

Lawyers are told by Comment [3] that if they use such services, they have to make “reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer’s professional obligations.” This extent of a lawyer’s efforts “will depend upon the circumstances.” However the following “circumstances” are specifically listed as ones that might be taken into account:

- “the education, experience and reputation of the nonlawyer”;
- “the nature of the services involved”;
- “the terms of any arrangements concerning the protection of client information”; ¹¹

¹⁰ Cf., e.g., Florida Ethics Op. 06-2 (http://www.floridabar.org/tfb/tfbetopin.nsf/SearchView/ETHICS+OPINION+06-2?opendocument) (citing to its comment identical to current Comment [6] of Model Rule 1.1, Florida RPC 4-1.1 “may necessitate a lawyer's continuing training and education in the use of technology in transmitting and receiving electronic information in order to protect client information under Rule 1.6(a).”)
• “the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality.”

Lawyers are also told by Comment [3] that they should communicate “directions appropriate under the circumstances to give reasonable assurance that the nonlawyer’s conduct is compatible with the professional obligations of the lawyer.” Prudent lawyers will do so in the form of a written agreement. 12

New Comment [4] addresses the client’s (as opposed to the lawyer’s) selection of the nonlawyer service provider. Invoking Model Rule 1.2, 13 it explains that where the client picks the third-party service provider, “the lawyer ordinarily should agree with the client concerning the allocation of responsibility for monitoring as between the client and the lawyer.” 14 In a report accompanying these changes to Model Rule 5.3, the Commission wrote that, “In such situations, the lawyer ordinarily

11 In a report accompanying this proposed Model Rule change, the Commission described what it had learned in the course of its investigation of measures taken to protect client information: “The Commission was particularly interested in procedures to protect confidential information. Although procedures vary depending on the type of work that is being outsourced, the Commission found that lawyer and nonlawyer employees of many outsourcing providers are required to sign confidentiality agreements, with some firms requiring employees to sign new and separate confidentiality agreements for each new assignment. Providers also frequently use security measures to protect electronic information (e.g., encryption, malware protection, firewalls). They use biometric and other security measures to ensure only authorized physical access to data, such as separate premises or areas for each project. They use continuous video monitoring, monitoring of employee computers, and repeated identity checks within buildings, elevators, and other areas where work is being performed. They frequently disable the portals on employee computers so that portable data storage devices cannot be used to remove information from the premises. They also perform extensive background checks on employees as well as periodic internal and external audits of all of the foregoing measures.”

12 In the report accompanying the proposed addition of comments to Model Rule 5.3, the Commission also discussed a third-party provider’s conflicts-of-interest: “The Commission found that conflict-of-interest considerations are increasingly given careful attention. For example, a number of outsourcing providers employ conflicts checking procedures modeled after those used by large U.S. and U.K. law firms; others are developing similar systems. These systems include maintaining extensive databases for existing and former clients and screening the work history of new recruits and existing employees against both the information contained in the databases and information supplied by the client.” The Commission also discussed the role of training: “The Commission’s research has revealed that a number of companies that provide outsourced services have established sophisticated training programs for nonlawyer and lawyer employees on a variety of topics, including U.S. substantive and procedural law, legal research and writing, and the rules of professional conduct. These companies also regularly seek input from and collaboration with the organized bar and lawyers and law firms in the development of ethics policies and training regimes for their lawyer and nonlawyer employees.” Lawyers using cloud-computing providers will need to evaluate both of these matters thoughtfully.

13 Model Rule 1.2(a) provides that a lawyer “shall abide by a client’s decisions concerning the objectives of representation” and, as required by Model Rule 1.4, “shall consult with the client as to the means by which they are to be pursued.” A lawyer can limit the scope of the representation “if the limitation is reasonable under the circumstances and the client gives informed consent.” Model Rule 1.2(c). Under Model Rule 1.2(d), “A lawyer shall not counsel a client to engage, or assist a client, in conduct that the lawyer knows is criminal or fraudulent, but a lawyer may discuss the legal consequences of any proposed course of conduct with a client and may counsel or assist a client to make a good faith effort to determine the validity, scope, meaning or application of the law.”

14 Proposed Comment [4] also states when a client and the lawyer allocate responsibility for monitoring the nonlawyer vendor, “lawyers and parties may have additional obligations that are a matter of law beyond the scope of these Rules.” In a separate report, the Commission explained this text “is intended to remind lawyers that they may have duties to a tribunal that are not necessarily satisfied through compliance with the Rules of Professional Conduct. For example, if a client instructs the lawyer to hire a particular electronic discovery vendor, the lawyer cannot cede all monitoring responsibility to the client, given that the lawyer may have to make certain representations to a tribunal regarding the vendor’s work.”
should consult with the client to determine how the outsourcing arrangement should be structured and who will be responsible for monitoring the performance of the nonlawyer services.”

The use of the word “monitoring” is new to the Model Rules. The Commission explained:

> The Commission concluded that [monitoring] was needed because, when a nonlawyer outside the firm is performing services in connection with a matter, it may not be possible to “directly supervise” the nonlawyer. The word “monitoring” makes clear that there is nevertheless a need to remain aware of how nonlawyer services are being performed. The Comment explains that, when the client directs the lawyer to use a particular nonlawyer, the lawyer and client should ordinarily agree who will have this “monitoring” responsibility. In contrast, if the client has not directed the selection of the nonlawyer, the lawyer or law firm would have the “monitoring” responsibility.

While these Model Rule amendments have now been adopted, state RPC are already being applied, without any rules changes, in the context of storage of data in a cloud-computing environment.

**STATE BAR ETHICS OPINIONS ON CLOUD COMPUTING/STORAGE**

The following state bar ethics opinions directly address cloud computing and cloud storage. In reading this discussion, lawyers should ask themselves whether the requirements contained in the opinions are manageable especially relative to the lawyer’s existing electronic storage practices and data security.

**Oregon Bar Ethics Opinion 2011-188 (November 2011)**

In November 2011, the Board of Governors of the Oregon Bar approved Formal Ethics Opinion 2011-18815 relating to “Third-Party Electronic Storage of Client Materials.” The Board determined that a lawyer may store client materials on a third-party vendor’s server “so long as the lawyer complies with the duties of competence and confidentiality to reasonably keep the client’s information secure within a given situation.”

What does that mean? Oregon lawyers must take “reasonable steps to ensure” that the cloud storage vendor “will reliably secure client data and keep information confidential.”

And what does that mean? The Oregon Ethics Committee does not say directly. Instead, the committee explains that “under certain circumstances” the duty to take reasonable steps to ensure the integrity and confidentiality of client data “may be satisfied” if the cloud storage vendor complies with “industry standards relating to confidentiality and security.” But there’s a catch. An Oregon lawyer

can rely on the vendor’s compliance with industry standards only if the industry standards “meet the minimum requirements imposed on the Lawyer by the Oregon RPCs.”

The only rules of professional conduct cited in the opinion are Oregon RPC 1.6 and 5.3. Those rules set performance standards: keep client information confidential with certain exceptions and take reasonable efforts to ensure that a person employed, retained, supervised, or directed by a lawyer acts consistent with the professional obligations of the lawyer. They do not provide specific requirements on how to meet these performance standards.

Using the words “may include,” the Oregon ethics committee authors do provide three suggestions for consideration by lawyers on how to meet the minimum requirements imposed on lawyers by the Oregon RPCs. The first of these merely transfers the lawyer’s performance standard to the vendor. In the agreement between the lawyer and the cloud storage vendor, the opinion contains the suggestion that the lawyer include a term that requires the vendor “to preserve the confidentiality and security of the materials.”

The second contains a more specific suggestion: requiring the vendor to notify the lawyer if the vendor’s storage server is hacked, i.e., that a “nonauthorized third-party” gains access to the materials.

The final suggestion relates to the lawyer’s evaluation of which cloud storage vendor to select. The opinion writers suggest that the lawyer “investigate how the vendor backs up and stores its data and metadata to ensure compliance with the Lawyer’s duties.”

Oregon Ethics Op. 2011-188 also addresses complacency. The authors explain that the reasonableness of the steps taken by the lawyer “will be measured against the technology ‘available at the time to secure data against unintentional disclosure.’ As technology advances, the third-party vendor’s protective measures may become less secure or obsolete over time.” Hence, the opinion’s writers conclude, a lawyer “may be required to reevaluate the protective measures used by the third-party vendor to safeguard the client materials.”

Formal Opinion 2011-188 ends on a sobering note: “A lawyer’s obligation in the event of a breach of security of confidential materials is outside the scope of this opinion.” Pennsylvania’s ethics opinion writers decided that much more was needed to guide lawyers in this potential ethics minefield.

---

16 In support of this suggestion, the authors refer to a 2005 Oregon ethics opinion dealing with a lawyer’s use of a recycling company for the proposition that the lawyer should instruct the vendor about the obligations imposed on a lawyer by Oregon RPC 1.6 and obtain the vendor’s agreement “to treat all materials appropriately.” Formal Opinion 2011-188, n. 3 (citing Oregon State Bar Formal Ethics Op. No. 2005-141 that can be found at http://www.osbar.org/_docs/ethics/2005-141.pdf).

Pennsylvania Formal Opinion 2011-200

In contrast with the Oregon State Bar’s minimalist approach, in its Ethics Op. 2011-200, the Pennsylvania Bar Association’s Ethics Committee decided on an expansive approach to address the ethics of cloud computing.

In rendering its opinion, the Pennsylvania Bar’s Ethics Committee focused on several rules of professional conduct: Rule 1.1 (competence); Rule 1.4 (communications with a client); Rule 1.6 (addressing confidentiality); Rule 1.15 (safeguarding client property); and Rule 5.3 (supervision of third parties). It specifically determined that a vendor must be “obligated to conform to the professional responsibilities required of lawyers, including a specific agreement to comply with all ethical guidelines” in the opinion. To obligate a vendor should require a written agreement, but the Pennsylvania Bar’s Ethics Committee only added that attorneys “may include” a written agreement with the cloud storage vendor “to protect the client’s interests.”

The Pennsylvania Ethics Committee introduced the role of informed consent in explaining that in some circumstances, “a client may need to be advised of the outsourcing or use of a service provider and the identification of the provider” and a lawyer “may also need an agreement or written disclosure with the client to outline the nature of the cloud services used, and its [sic] impact upon the client’s matter.” The Committee also focused on the lawyer’s lack of direct control over a cloud storage vendor, the potential for advances in technology that can affect professional conduct standards for lawyers storing data in the cloud, interruptions in service, and loss of data.19

It then undertook to create a checklist for lawyers against which the “standard of reasonable care” for cloud computing would be measured. The Pennsylvania Ethics Committee wrote that “the standard of reasonable care for ‘cloud computing’ may include” the following issues or recommendations. I have categorized the long list of both in the following table. The Pennsylvania opinion is remarkable for the level of detail it provides to tell lawyers what factors might determine not whether a lawyer is complying with ethics rules but whether a lawyer is meeting the “standard of reasonable care”:

<table>
<thead>
<tr>
<th>Category</th>
<th>Issue or Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity of original data</td>
<td>• Backing up data to allow the firm to restore data that has been lost, corrupted, or accidentally deleted.</td>
</tr>
<tr>
<td>Unauthorized third party access</td>
<td>• Install a firewall to limit access to the firm’s network.</td>
</tr>
<tr>
<td></td>
<td>• Refuse to disclose confidential information to unauthorized individuals (including family members and friends) without client permission.</td>
</tr>
</tbody>
</table>


19 The Pennsylvania Ethics Committee gave these examples: “Amazon EC2 has experienced outages in the past few years, leaving a portion of users without service for hours at a time. Google has also had multiple service outages, as have other providers. Digital Railroad, a photo archiving service, collapsed financially and simply shut down. These types of risks should alert anyone contemplating using cloud services to select a suitable provider, take reasonable precautions to back up data and ensure its accessibility when the user needs it.”
<table>
<thead>
<tr>
<th>Category</th>
<th>Issue or Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Implement electronic audit trail procedures to monitor who is accessing the data.</td>
</tr>
<tr>
<td></td>
<td>• Have technology in place built to withstand a reasonably foreseeable attempt to infiltrate data, including penetration testing.</td>
</tr>
<tr>
<td>Confidentiality/Security</td>
<td>• Have a written agreement to enforce the provider’s obligation to preserve security.</td>
</tr>
<tr>
<td></td>
<td>• Verify the identity of individuals to whom the attorney provides confidential information.</td>
</tr>
<tr>
<td></td>
<td>• Limit information that is provided to others to what is required, needed, or requested.</td>
</tr>
<tr>
<td></td>
<td>• Protect electronic records containing confidential data, including backups by encrypting the confidential data.</td>
</tr>
<tr>
<td></td>
<td>• Avoid inadvertent disclosure of information.</td>
</tr>
<tr>
<td></td>
<td>• Include in a “Terms of Service” or “Service Level Agreement” terms addressing how confidential client information will be handled.</td>
</tr>
<tr>
<td></td>
<td>• Create plans to address security breaches, including the identification of persons to be notified about any known or suspected security breach involving confidential data.</td>
</tr>
<tr>
<td>Data Ownership</td>
<td>• The provider explicitly agrees that it has no ownership or security interest in the data and that the Service Level Agreement “clearly states that the attorney owns the data.”</td>
</tr>
<tr>
<td>Review Rights Before</td>
<td>• If requested, the provider will notify the lawyer to give the lawyer the ability to respond to the request before the provider produces requested information.</td>
</tr>
<tr>
<td>Releasing Data</td>
<td></td>
</tr>
<tr>
<td>Audit Rights</td>
<td>• The lawyer has a right to audit the provider’s security procedures and to obtain copies of any security audits performed by others.</td>
</tr>
<tr>
<td>Host Server Location</td>
<td>• The provider will host the firm’s data only within a specified geographical area. “If by agreement, the firm’s data are hosted outside of the United States, the law firm must determine that the</td>
</tr>
</tbody>
</table>

---

20 The opinion later notes that at least 45 states, including Pennsylvania, have adopted data breach notification laws. In Pennsylvania, for example, 73 P.S. § 2303 (2011) provides that a vendor that maintains, stores, or manages computerized data on behalf of another entity “shall provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data. The entity shall be responsible for making the determinations and discharging any remaining duties under this act.” Those duties include: “notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Except as provided in section 4 or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay. For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.” Id. It is unclear how this law would apply to a Pennsylvania lawyer’s corporate client that is not incorporated in Pennsylvania or does not have its principal place of business in Pennsylvania.
<table>
<thead>
<tr>
<th>Category</th>
<th>Issue or Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure that are as rigorous as those of the United States and Pennsylvania.”</td>
</tr>
<tr>
<td>Termination</td>
<td>• The provider must provide “a method of retrieving data if the lawyer terminates use” of the SaaS (software as a service) product, “the SaaS vendor goes out of business, or the service otherwise has a break in continuity.”</td>
</tr>
<tr>
<td>Training</td>
<td>• Employees of the law firm who use the SaaS must receive appropriate training.</td>
</tr>
<tr>
<td>Compliance With Data Protection Measures</td>
<td>• Employees who use the SaaS are required to abide by all end-user measures, including, but not limited to, the creation of strong passwords and the regular replacement of passwords.</td>
</tr>
<tr>
<td>Copies of Data</td>
<td>• To protect “the ability to represent the client reliably,” the law firm should consider “ensuring that a copy of digital data is stored onsite.” The authors add a footnote saying that “this is recommended even though many vendors will claim that it is not necessary.”</td>
</tr>
<tr>
<td>Lawyer Due Diligence</td>
<td>Investigating the provider’s:</td>
</tr>
<tr>
<td></td>
<td>• security measures, policies and recovery methods;</td>
</tr>
<tr>
<td></td>
<td>• system for backing up data;</td>
</tr>
<tr>
<td></td>
<td>• security of data centers and whether the storage is in multiple centers;</td>
</tr>
<tr>
<td></td>
<td>• safeguards against disasters, including different server locations;</td>
</tr>
<tr>
<td></td>
<td>• history, including how long the provider has been in business;</td>
</tr>
<tr>
<td></td>
<td>• funding and stability;</td>
</tr>
<tr>
<td></td>
<td>• policies for data retrieval upon termination of the relationship and any related charges;</td>
</tr>
<tr>
<td></td>
<td>• process to comply with data that is subject to a litigation hold; and</td>
</tr>
<tr>
<td></td>
<td>• use of third-party audits of security.</td>
</tr>
<tr>
<td>Data Format</td>
<td>• Determining whether data is stored in a nonproprietary format.</td>
</tr>
<tr>
<td>Retrieval of Data When Needed For Use Offline</td>
<td>• Provide the ability for the law firm to get data “off” of the vendor’s or third-party data hosting company’s servers for the firm’s own use or in-house backup offline.</td>
</tr>
<tr>
<td>Internet Connectivity</td>
<td>• Because cloud service is accessible only through the Internet, in the event of an Internet access failure at the law firm, having an alternate way for the law firm to connect to the Internet cloud service.</td>
</tr>
<tr>
<td>Credits</td>
<td>• The provider gives the lawyer a guarantee of the “uptime” or the likelihood that the cloud server can be accessed close to 100% of the time, and states whether failure to achieve promised uptime will result in service credits to the lawyer on behalf of the lawyer’s client.</td>
</tr>
</tbody>
</table>
The authors of Pennsylvania Ethics Op. 2011-200 did not stop here, however. They also explained that most Service Level Agreements with cloud storage vendors are typically “take it or leave it” offers of service and they add that “often users, including lawyers, do not read the terms closely or at all.” After this indictment of some members of the Pennsylvania Bar, they add:

As a result, compliance with ethical mandates can be difficult. However, new competition in the “cloud computing” field is now causing vendors to consider altering terms. This can help attorneys meet their ethical obligations by facilitating an agreement with a vendor that adequately safeguards security and reliability.

In the same breath, the authors caution lawyers against “upstart providers” who “may not have staying power.”

Because security is so critical, the opinion also contains the suggestion that “incident response plans” should be in place before attorneys begin using cloud services and that these plans should be reviewed “annually.” The opinion’s authors also suggest that lawyers consider whether or not some data “may be too important to risk inclusion in cloud services.” The inference here, presumably, is that such data is otherwise well protected from a security breach.

Pennsylvania Ethics Op. 2011-200 contains this conclusion in pertinent part:

This Committee concludes that the Pennsylvania Rules of Professional Conduct require attorneys to make reasonable efforts to meet their obligations to ensure client confidentiality, and confirm that any third-party service provider is likewise obligated.

Accordingly, as outlined above, this Committee concludes that, under the Pennsylvania Rules of Professional Conduct, an attorney may store confidential material in “the cloud.” Because the need to maintain confidentiality is crucial to the attorney-client relationship, attorneys using “cloud” software must take appropriate measures to protect confidential electronic communications and information.

The authors of the opinion cataloged ethics opinions from 13 other state bars on the issue of storing client files. One of the opinions listed was Proposed Formal Opinion 6 issued April 21, 2011 by a subcommittee to the North Carolina State Bar Ethics Committee. The Pennsylvania opinion “adopts in large part the recommendations” of this proposed opinion, which has now been adopted by the full North Carolina Bar Ethics Committee.

The North Carolina Bar’s Ethics Committee issued 2011 Formal Opinion 6\(^2\) in response to an inquiry from a law firm as to whether or not it could use “software as a service” for computing in a cloud environment. The inquiry was framed as follows:

*SaaS for law firms may involve the storage of a law firm’s data, including client files, billing information, and work product, on remote servers rather than on the law firm’s own computer and, therefore, outside the direct control of the firm’s lawyers. Lawyers have duties to safeguard confidential client information, including protecting that information from unauthorized disclosure, and to protect client property from destruction, degradation, or loss (whether from system failure, natural disaster, or dissolution of a vendor’s business). Lawyers also have a continuing need to retrieve client data in a form that is usable outside of a vendor’s product.

Given these duties and needs, may a law firm use SaaS?

Relying on RPC 1.6 and 1.15, the proposed opinion answered this question, “Yes” with the following caveats:

1. The lawyer had to take steps “to minimize the risk of inadvertent or unauthorized disclosure of confidential client information and to protect client property, including the information in a client’s file, from risk of loss.”

2. The lawyer must protect against Internet security weaknesses, “particularly ‘end-user’ vulnerabilities found in the lawyer’s own law office.”

3. The lawyer must engage “in periodic education about ever-changing security risks” presented by the Internet.

4. “A lawyer must fulfill the duties to protect confidential client information and to safeguard client files by applying the same diligence and competency to manage the risks of SaaS that the lawyer is required to apply when representing clients.”

In a second inquiry, the law firm asked whether there were “measures that a lawyer or law firm should consider when assessing a SaaS vendor or seeking to minimize the security risks of SaaS?”

The authors of the proposed opinion elected not to identify “specific security requirements” because the security risk dynamics are too fluid. “Instead, due diligence and frequent and regular education are required.”

Nonetheless, in the context of a lawyer’s supervisory obligations under RPC 5.3(a), the authors opined that the extent of these obligations “when using a SaaS vendor to store and manipulate confidential client information will depend upon the experience, stability, and reputation of the vendor. Given the rapidity with which computer technology changes, law firms are encouraged to consult periodically

with professionals competent in the area of online security.” The opinion then contained five “recommended security measures”:

1. Inclusion in the SaaS vendor’s Terms of Service or Service Level Agreement of terms on how the vendor “will handle confidential client information in keeping with the lawyer’s professional responsibilities.”

2. “If the lawyer terminates use of the SaaS product, the SaaS vendor goes out of business, or the service otherwise has a break in continuity, the law firm will have a method for retrieving the data, the data will be available in a non-proprietary format that the law firm can access, or the firm will have access to the vendor’s software or source code. The SaaS vendor is contractually required to return or destroy the hosted data promptly at the request of the law firm.”

3. “Careful review of the terms of the law firm’s user or license agreement with the SaaS vendor including the security policy.”

4. “Evaluation of the SaaS vendor’s (or any third party data hosting company’s) measures for safeguarding the security and confidentiality of stored data including, but not limited to, firewalls, encryption techniques, socket security features, and intrusion-detection systems.”

5. “Evaluation of the extent to which the SaaS vendor backs up hosted data.”

According to one blogger, the Legal Cloud Computing Association had submitted the following comment against adoption of the opinion in its proposed form because the requirements recommended were too onerous:

[W]e believe that the additional minimum requirements imposed on lawyers as mandatory requirements will, as a practical matter, limit the ability of North Carolina lawyers to use cloud computing services in their practices, causing North Carolina’s lawyers to become less competitive with lawyers from other states.

Rather than “mandatory requirements”, we believe that it makes more sense to establish basic principles and suggested guidelines, leaving to the individual attorney to use their [sic] best judgment to exercise reasonable care under the particular circumstances of their [sic] practice, in choosing a SaaS provider.

While comments like these delayed the final decision of the North Carolina’s Ethics Committee, 2011 Formal Opinion 6 was adopted in substantially the same form as it was proposed.

22 In a footnote, the North Carolina Ethics subcommittee explained how it was using these terms: “A firewall is a system (which may consist of hardware, software, or both) that protects the resources of a private network from users of other networks. Encryption techniques are methods for ciphering messages into a foreign format that can only be deciphered using keys and reverse encryption algorithms. A socket security feature is a commonly-used protocol for managing the security of message transmission on the Internet. An intrusion detection system is a system (which may consist of hardware, software, or both) that monitors network and/or system activities for malicious activities and produces reports for management.”

New York State Bar Ethics Opinion 842 (Sept. 10, 2010)

New York’s State Bar weighed in on this topic in 2010 with NY State Bar Ethics Op. 842, a more general opinion, unlike the Pennsylvania or North Carolina opinions that contained several specific recommendations. New York’s RPC 1.6 is also different from Model Rule 1.6 and the Pennsylvania and North Carolina versions of Model Rule 1.6 because it contains a unique provision that establishes a duty on a lawyer when utilizing the services of others to use “reasonable care” to protect the confidentiality of client information. NY RPC 1.6(c) provides: “A lawyer shall exercise reasonable care to prevent the lawyer’s employees, associates, and others whose services are utilized by the lawyer from disclosing or using confidential information of a client, except that a lawyer may reveal the information permitted to be disclosed by paragraph (b) through an employee.”

Against this ethical backdrop, the New York State Bar Ethics Committee explained that “a lawyer may use online ‘cloud’ computer data backup system to store client files provided that the lawyer takes reasonable care to ensure that the system is secure and that client confidentiality will be maintained.” The committee then determined that “reasonable care” to protect a client’s confidential information against unauthorized disclosure “may include” consideration of these steps:

1. Ensuring that the cloud-storage provider “has an enforceable obligation to preserve confidentiality and security; and that the provider will notify the lawyer if served with process requiring the production of client information.”
2. Investigating the cloud-storage provider’s “security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances.”
3. “Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored.”
4. “Reconfirming that the provider’s security measures remain effective in light of advances in technology.”

The committee also opined that if a lawyer learns information “suggesting that the security measures” used by the cloud-storage provider “are insufficient to adequately protect the confidentiality of client information, or if the lawyer learns of any breach of confidentiality by the online-storage provider, then the lawyer must investigate whether there has been any breach of his or her own clients’ confidential information, notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated.”

Alabama Ethics Opinion 2010-02

In Ethics Op. 2010-02 the Alabama Bar Ethics Committee addressed a number of questions relating to storage of information. With respect to cloud-based storage, the committee noted the “obvious

http://www.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&CONTENTID=42697&TEMPLATE=/CM/ContentDisplay.cfm
“The duty of reasonable care requires the lawyer to become knowledgeable about how the provider will handle the storage and security of the data being stored and to reasonably ensure that the provider will abide by a confidentiality agreement in handling the data.”

2. Because “technology is constantly evolving, the lawyer will have a continuing duty to stay abreast of appropriate security safeguards that should be employed by the lawyer and the third-party provider.”

3. The storage format “must allow the lawyer to reproduce the documents in their original paper format.”

4. If the client requests a copy of electronically stored files, “the lawyer must abide by the client’s decision in whether to produce the file in its electronic format, such as on a compact disc or in its original paper format.”

Washington State Bar Advisory Opinion 2215 (2012)

In Advisory Opinion 2215, the Washington State Bar RPC Committee acknowledged that lawyers may be interested in using cloud computing to store confidential client documents and other data even though such use eliminates direct control by the lawyer of client information. Citing Washington RPC 1.6, 1.1, 5.1, 5.3 and 1.15A, the Committee determined that a lawyer has a duty both to maintain client confidentiality and to ensure that client data are not lost. Because “technology is changing too rapidly,” the Committee said it was “impossible” to give specific guidelines on security measures that would always be applicable in the future.

But the Committee did admonish lawyers that they must conduct “a due diligence investigation of the provider and its services and cannot rely on lack of technological sophistication to excuse the failure to do so.” To help such lawyers, however, the Committee added that “best practices for a lawyer without advanced technological knowledge could include” the following seven ideas:

26 The committee added: “If there is a breach of confidentiality, the focus of any inquiry will be whether the lawyer acted reasonably in selecting the method of storage and/or the third party provider.”

1. Familiarization with the potential risks of online data storage and review of available general audience literature and literature directed at the legal profession, on cloud computing industry standards and desirable features.
2. Evaluation of the provider’s practices, reputation and history.
3. Comparison of provisions in service provider agreements to the extent that the service provider recognizes the lawyer’s duty of confidentiality and agrees to handle the information accordingly.
4. Comparison of provisions in service provider agreements to the extent that the agreement gives the lawyer methods for retrieving the data if the agreement is terminated or the service provider goes out of business.
5. Confirming provisions in the agreement that will give the lawyer prompt notice of any nonauthorized access to the lawyer’s stored data.
6. Ensure secure and tightly controlled access to the storage system maintained by the service provider.
7. Ensure reasonable measures for secure backup of the data that is maintained by the service provider.

The Committee also explained that to remain “competent” under Washington RPC 1.1, a lawyer has a duty “to keep informed about the risks associated with that technology and to take reasonable precautions.” Saying that the duties on a lawyer in this context are not a “guarantee” of security from unauthorized access, and noting that security breaches are possible in the “physical world” too, the Committee explained that a lawyer “has always been under a duty to make reasonable judgments when protecting client property and information. Specific practices regarding protection of client property and information have always been left up to individual lawyers’ judgment, and that same approach applies to the use of online data storage. The lawyer must take reasonable steps, however, to evaluate the risks involved with that practice and to ensure that steps taken to protect the information are up to a reasonable standard of care.”

Finally, the Committee noted that because technology changes rapidly, a lawyer must “monitor and regularly review the security measures of the provider” because “[o]ver time, a particular provider’s security may become obsolete or become substandard to systems developed by other providers.”

**Iowa Bar Ethic Opinion 11-01 (September 9, 2011)**

The Iowa State Bar Committee on Ethics and Practice Guidelines issued Opinion 11-01 approved the use of SaaS to store client information under Iowa RPC 1.6 with the caveat that lawyers have the obligation to perform due diligence “to assess the degree of protection that will be needed and to act accordingly.” The Committee gave “basic guidance” regarding the lawyer’s obligations by identifying questions to ask in the areas of “accessibility” and “data protection” as reflected in the following table:

---

<table>
<thead>
<tr>
<th>Topic</th>
<th>Accessibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>“Will I have unrestricted access to the stored data? Have I stored the data elsewhere so that if access to my data is denied I can acquire the data via another source?”</td>
</tr>
<tr>
<td>Legal Issues</td>
<td>“Have I performed ‘due diligence’ regarding the company that will be storing my data? Are they a solid company with a good operating record and is their service recommended by others in the field? What country and state are they located and do business in? Does their end user’s licensing agreement (EULA) contain legal restrictions regarding their responsibility or liability, choice of law or forum, or limitation on damages? Likewise does their EULA grant them proprietary or user rights over my data?”</td>
</tr>
<tr>
<td>Financial Obligation</td>
<td>“What is the cost of the service, how is it paid and what happens in the event of non-payment? In the event of a financial default will I lose access to the data, does it become the property of the SaaS company or is the data destroyed?”</td>
</tr>
<tr>
<td>Termination</td>
<td>“How do I terminate the relationship with the SaaS company? What type of notice does the EULA require. How do I retrieve my data and does the SaaS company retain copies?”</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Topic</th>
<th>Data Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Protection and Public Access</td>
<td>“Are passwords required to access the program that contains my data? Who has access to the passwords? Will the public have access to my data? If I allow non-clients access to a portion of the data will they have access to other data that I want protected?”</td>
</tr>
<tr>
<td>Data Encryption</td>
<td>“Recognizing that some data will require a higher degree of protection than others, will I have the ability to encrypt certain data using higher level encryption tools of my choosing?”</td>
</tr>
</tbody>
</table>

**Vermont Ethics Opinion 2010-6**

The Vermont Bar Ethics Committee addressed utilization of SaaS in Opinion 2010-6. In a familiar refrain, the Committee cited Vermont RPC 1.6, 1.1, 1.15, and 5.3 as the backdrop for its discussion. It also quoted from or cited to ethics opinions from North Carolina (Proposed Formal Opinion No. 6), Iowa (11-01), Pennsylvania (Formal Opinion 2011-200), New York (NYSBA Opinion 842), Alabama

---

29 [https://www.vtbar.org/FOR%20ATTORNEYS/Advisory%20Ethics%20Opinion.aspx](https://www.vtbar.org/FOR%20ATTORNEYS/Advisory%20Ethics%20Opinion.aspx)
(Opinion 2010-02) discussed above, and California (2010-179), Arizona (Opinion 90-04), New Jersey (Opinion 701), and Nevada (Opinion No. 33) discussed below.

After completing this survey, the Committee agreed that lawyers may use SaaS for storing, processing, and retrieving client property but, in doing so, the focus of lawyers must be on competence, confidentiality, and security. It recognized that cloud computing is a dynamic area and thus it would not be prudent to establish “specific conditions precedent to using SaaS.” Instead, Vermont lawyers must exercise due diligence when using cloud computing. What does that mean? The Committee referenced examples of check list items from the opinions it cited but then said that “[c]omplying with the required level of due diligence will often involve a reasonable understanding of” the following:

a. the vendor’s security system;

b. what practical and foreseeable limits, if any, may exist to the lawyer’s ability to ensure access to, protection of, and retrieval of the data;

c. the material terms of the user agreement;

d. the vendor’s commitment to protecting confidentiality of the data;

e. the nature and sensitivity of the stored information;

f. notice provisions if a third party seeks or gains (whether inadvertently or otherwise) access to the data; and

g. other regulatory, compliance, and document retention obligations that may apply based upon the nature of the stored data and the lawyer’s practice.

In addition, the lawyer should consider:

a. giving notice to the client about the proposed method for storing client data;31

b. having the vendor’s security and access systems reviewed by competent technical personnel;

c. establishing a system for periodic review of the vendor’s system to be sure the system remains current with evolving technology and legal requirements; and

30 The opinion provides: “[I]t may not be appropriate to rely solely on remote digital storage for preservation of original client property like wills, or other client documents that are subject to permanent retention obligations. Similarly, given that Cloud Computing involves storage of information in the hands of a third party, a lawyer handling particularly sensitive client property, like trade secrets may conclude after consultation with the client that remote SaaS storage is not sufficiently secure.”

31 Giving notice to the client is something a lawyer should “consider”; it is not mandated. However, for trade secrets and other sensitive client information presumably under lock and key or its equivalent in physical storage by the lawyer, a lawyer is well-advised to consult with the client before moving the information to a cloud storage environment where it may be less secure.
d. taking reasonable measures to stay apprised of current developments regarding SaaS systems and the benefits and risks they present.

The Committee added that the “ability to engage in Cloud Computing is not limited by the specific location of the remote server, although some of the factors noted above, including choice of law clauses, and concerns about access to data in the event of a service interruption or an emergency, may be implicated by the location of the storage server and the extent of backup service provided by the vendor.”

The Committee added that a lawyer’s “use of email, calendar, and remote synchronization systems, including systems that are web-based and offered by SaaS vendors, is subject to the same inquiry. Before using such systems, the lawyer should take reasonable precautions to ensure that information in the system is secure and accessible.”

Massachusetts Bar Ethics Opinion 12-03 (May 17, 2012)

Massachusetts Bar Ethics Opinion 12-03\(^{32}\) contains this summary of its determination:

A lawyer generally may store and synchronize electronic work files containing confidential client information across different platforms and devices using an Internet based storage solution, such as “Google docs,” so long as the lawyer undertakes reasonable efforts to ensure that the provider’s terms of use and data privacy policies, practices and procedures are compatible with the lawyer’s professional obligations, including the obligation to protect confidential client information reflected in Rule 1.6(a). A lawyer remains bound, however, to follow an express instruction from his or her client that the client’s confidential information not be stored or transmitted by means of the Internet, and all lawyers should refrain from storing or transmitting particularly sensitive client information by means of the Internet without first obtaining the client’s express consent to do so.

What are reasonable efforts to ensure that the cloud computing vendor’s practices are compatible with the lawyers’ professional obligations? The Committee offered five possible steps lawyers could take:

1. “examining the provider’s terms of use and written policies and procedures with respect to data privacy and the handling of confidential information;”
2. “ensuring that the provider’s terms of use and written policies and procedures prohibit unauthorized access to data stored on the provider’s system, including access by the provider itself for any purpose other than conveying or displaying the data to authorized users;”
3. “ensuring that the provider’s terms of use and written policies and procedures, as well as its functional capabilities, give the Lawyer reasonable access to, and control over, the data stored on the provider’s system in the event that the Lawyer’s relationship with the provider is interrupted

for any reason (e.g., if the storage provider ceases operations or shuts off the Lawyer’s account, either temporarily or permanently)

4. “examining the provider’s existing practices (including data encryption, password protection, and system back ups) and available service history (including reports of known security breaches or “holes”) to reasonably ensure that data stored on the provider’s system actually will remain confidential, and will not be intentionally or inadvertently disclosed or lost;” and

5. “periodically revisiting and reexamining the provider’s policies, practices and procedures to ensure that they remain compatible with Lawyer’s professional obligations to protect confidential client information reflected in Rule 1.6(a).”

Relying on prior opinions it had issued, the Committee added that it believed that a lawyer remains bound “to follow an express instruction from his client that the client’s confidential information not be stored or transmitted by means of the Internet, and that he should refrain from storing or transmitting particularly sensitive client information by means of the Internet without first seeking and obtaining the client’s express consent to do so.”

New Hampshire Ethics Committee Advisory Opinion #2012-13/4

In Advisory Ethics Op. #2012-13/4, the New Hampshire Bar’s Ethics Committee also approved a lawyer’s use of cloud computing with the same caveats offered in other ethics’ opinions on this topic.33

The committee first discussed the applicable RPC. In its discussion of RPC 1.1, the committee referenced the change to Comment [6] to Model Rule 1.1, stating that lawyers must keep abreast of changes “in the law and its practice, including the benefits or risks associated with relevant technology.” The committee stated bluntly: “A competent lawyer using cloud computing must understand and guard against the risks inherent in it.” It also admonished: “Competent lawyers must have a basic understanding of the technologies they use.”

The committee also referenced the changes to Model Rule 1.6 explaining that, “As cloud computing comes into wider use, storing and transmitting information in the cloud may be deemed an impliedly authorized disclosure to the provider, so long as the lawyer takes reasonable steps to ensure that the provider of cloud computing services has adequate safeguards.” Informed consent from a client “may be necessary,” if information stored in the cloud is “highly sensitive,” the committee added.

Citing RPC 1.15 and 1.16(d), the committee established this framework for safeguarding and return of client property: “a lawyer must take reasonable steps to ensure that electronic data stored in the cloud is secure and available while representing a client. The data must be returned to the client and deleted from the cloud after representation is concluded or when the lawyer decides to no longer to preserve the file: in either case, the lawyer must know at all times where sensitive client information is stored, be it in the cloud or elsewhere.”

Explaining that a provider of cloud computing services is “in effect” a nonlawyer retained by a lawyer, the committee invoked RPC 5.3(a) to remind lawyers of their supervisory obligations, whether the lawyer hires the provider directly or through an intermediary. In the latter case, the committee also invoked RPC 2.1 to also remind lawyers that they “must exercise independent professional judgment in representing a client and cannot hide behind a hired intermediary and ignore how client information is stored in or transmitted through the cloud.” In a mollifying statement, however, the committee also pointed out that lawyers are not guarantors of the conduct of third parties: “It bears repeating that a lawyer’s duty is to take reasonable steps to protect confidential client information, not to become an expert in information technology. When it comes to the use of cloud computing, the Rules of Professional Conduct do not impose a strict liability standard.”

The committee then summarized issues a lawyer “must consider” before using a cloud computing service. They “include the following”:

1. Is the provider of cloud computing services a reputable organization?

2. Does the provider offer robust security measures? Such measures must include at a minimum password protections or other verification procedures limiting access to the data; safeguards such as data back-up and restoration, a firewall, or encryption; periodic audits by third parties of the provider’s security; and notification procedures in case of a breach.

3. Is the data stored in a format that renders it retrievable as well as secure? Is it stored in a proprietary format and is it promptly and reasonably retrievable by the lawyer in a format acceptable to the client? (Citation omitted.) It bears repeating that, if a client requests a copy of her file, the lawyer has an obligation to provide all files pertinent to representation of that client. (Citations omitted.)

4. Does the provider commingle data belonging to different clients and/or different practitioners such that retrieval may result in inadvertent disclosure?

5. Do the terms of service state that the provider merely holds a license to the stored data, as for example Google’s do? Some providers routinely inform those accessing their service that it is the provider—not the user—that “owns” the data. If the

---

34 Model Rule 2.1 and New Hampshire RPC 2.1 both provide: “In representing a client, a lawyer shall exercise independent professional judgment and render candid advice. In rendering advice, a lawyer may refer not only to law but to other considerations such as moral, economic, social and political factors, that may be relevant to the client’s situation.”


36 All footnotes are omitted, but most of references cited by the committee were the cloud computing opinions from Pennsylvania and Iowa discussed earlier.
provider owns the stored data, the lawyer may run afoul of Rule 1.15, which requires that the client’s property “be identified as property of the client.” To comply with Rule 1.15, the provider may not “own” the data stored in the cloud.

6. Does the provider have an enforceable obligation to keep the data confidential?

7. Where are the provider’s servers located and what are the privacy laws in effect at that location regarding unauthorized access, retrieval, and destruction of compromised data? If the servers are located in a foreign country, do the privacy laws of that country reasonably mirror those of the United States? If the servers are relocated, will the provider notify the lawyer in advance?

8. Will the provider retain the data – and, if so, for how long – when the representation ends or the agreement between the lawyer and provider is terminated for another reason? The data must not be destroyed immediately and without notice or compromised in case of nonpayment.

9. Do the terms of service obligate the provider to warn the lawyer if information is being subpoenaed by a third party, where the law permits such notice?\(^{37}\)

10. What is the provider’s disaster recovery plan with respect to stored data? Is a copy of the digital data stored on-site?


The committee was quite forceful in its conclusion:

Granted, a lawyer may not find a provider of cloud computing services whose terms of service address all of the issues addressed above, but it bears repeating, that while a lawyer need not become an expert in data storage, a lawyer must remain aware of how and where data is stored and what the service agreement says. Although the New Hampshire Rules of Professional Conduct do not impose a strict liability standard, the duties of confidentiality and competence are ongoing and not delegable. The requirement of competence means that even when storing data in the cloud, a lawyer must take reasonable steps to protect client information and cannot allow the storage and retrieval of data to become nebulous.

*Id.* (Footnote omitted.)

---

\(^{37}\) Here, the committee added: “Such a provision may be especially timely given that the Senate Judiciary Committee recently considered, but rejected legislation which would have expanded law enforcement agencies’ access to privately stored data.”
The Professional Ethics Committee of the Florida Bar has issued a proposed opinion on cloud computing in response to a direction from the Florida Bar Board of Governors. Citing to Florida RPC 4-1.6 and its prior opinions, the committee first explained that Florida lawyers (1) have a duty to ensure that confidentiality of client information is maintained by nonlawyers under their supervision, and (2) “have an ethical obligation to understand the technology they are using and how it potentially impacts confidentiality of information relating to client matters, so that the lawyers may take appropriate steps to comply with their ethical obligations.”

Then, citing to other state bar ethics opinions approving cloud computing or remote storage of electronic data, the committee focused on the appropriate level of due diligence required of a lawyer and practical issues associated with access. It endorsed the due diligence steps set forth in New York State Bar Ethics Opinion 842 as well as the practical advice contained in Iowa Ethics Opinion 11-01, both discussed above. It concluded with one more recommendation where highly sensitive information is involved, and before providing a summary of its conclusion:

Additionally, this Committee believes that the lawyer should consider whether the lawyer should use the outside service provider or use additional security in specific matters in which the lawyer has proprietary client information or has other particularly sensitive information.

In summary, lawyers may use cloud computing if they take reasonable precautions to ensure that confidentiality of client information is maintained. The lawyer should research the service provider to be used, should ensure that the service provider maintains adequate security, should ensure that the lawyer has adequate access to the information stored remotely, and should consider backing up the data elsewhere as a precaution.

STATE BAR ETHICS OPINIONS ON REMOTE STORAGE OF ELECTRONIC DATA

In my book, The Ethics of E-Discovery (p. 46-58), I discuss a number of ethics opinions that address generally the topic of electronic storage of client data. Three ethics opinions on storage of client data rendered since The Ethics of E-Discovery was published have relevance to the ethics of cloud storage.

California State Bar Standing Committee on Professional Responsibility and Conduct Formal Opinion 2010-179

California does not follow the Model Rules of Professional Conduct. However, its Ethics Op. 2010-179, while not dealing specifically with cloud computing, reaches similar conclusions under 38


39 http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmcEClHp7h4%3D&tabid=837
California Rules of Professional Conduct in examining the analysis an attorney should undertake “when considering use of a particular form of technology.”

The committee focused on the duty of confidentiality and competence and a lawyer’s supervisory obligations in identifying the following as some of the factors that a lawyer should consider before adopting a particular technology: (a) the level of security associated with the technology; (b) whether the technology allows users to take steps to increase the level of security; (c) what limitations there are on controlling access to electronic information, particularly confidential information; (d) the degree of sensitivity of the information; (e) the impact on the client of an inadvertent disclosure of privileged or confidential information or work product; and (f) the client’s instructions and circumstances.

**Illinois State Bar Association Advisory Opinion 10-01 (July 2009)**

ISBA Ethics Op. 10-01 does not address cloud computing directly but is still relevant to the topic. The question presented involved a law firm that wanted to have its computer network managed by a third-party vendor in an off-site location. The vendor would have access to the data on the system to administer the computer system but the law firm and the vendor “would enter into a written agreement whereby the vendor would agree to respect and maintain the confidentiality of the information within the network, and to not utilize or disclose it.”

Relying on RPC 1.6 and 5.3, ISBA Ethics Op. 10-01 states that “a law firm may retain or work with a private vendor to monitor the firm’s computer server and network, either on-site or remotely, and may allow the vendor to access it as needed for maintenance, updating, troubleshooting and similar purposes. Before doing so, however, the law firm must take reasonable steps to ensure that the vendor protects the confidentiality of the clients’ information on the server.”

The only additional wisdom that can be extracted from the opinion is that the law firm should (a) examine the vendor’s existing policies and procedures with respect to the handling of confidential information; (b) secure a written agreement from the vendor to protect confidential data; and (c) if the vendor breaches this duty, consider whether the law firm has to disclose this breach to its client if the breach “is likely to affect the position of the client or the outcome of the client’s case.”

**Arizona Ethics Opinion 09-04**

Arizona Ethics Op. 09-04 sought to answer the following question: May a lawyer “maintain an encrypted online file storage and retrieval system for clients in which all documents are converted to password-protected PDF format and stored in online folders with unique, randomly-generated alphanumeric names and passwords”?

---

Relying on earlier Arizona ethics opinion, RPC 1.1 and 1.6, and ethics opinions from other state bar associations, the Arizona Bar Ethics Committee explained that lawyers moving into online storage should get assistance: “The competence requirements of ER 1.1 apply not only to a lawyer’s legal skills, but also generally to ‘those matters reasonably necessary for the representation.’ Therefore, as a necessary prerequisite to making a determination regarding the reasonableness of online file security precautions, the lawyer must have, or consult someone with, competence in the field of online computer security.”

The committee then held that the lawyer making the inquiry “appears” to meet the requirements of Arizona’s RPC because:

1. The files would be protected by a Secure Socket Layer server, which encrypts the files.
2. There were “several layers of password protection.”
3. The filing system “utilizes unique and randomly generated folder names and passwords.”
4. Each document was converted to PDF format and requires another unique alpha-numeric password before it can be reviewed.

Because of advances in technology, the committee added that “lawyers should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients’ documents and information.”

**New Jersey Ethics Opinion 701 (2006)**

In New Jersey Ethics Opinion 701, the New Jersey Bar Ethics Committee answered the question of whether the New Jersey RPC permitted a lawyer to scan client documents into a digitized format such as Portable Data Format (“PDF”) for storage electronically so that they can be “sent by email” or retrieved “from any location in the world.” The inquiring lawyer noted that, “certain documents that by their nature require retention of original hardcopy, such as wills, and deeds, would be physically maintained in a separate file.”

The Committee approved of the procedure. However, it determined that (1) a lawyer must use reasonable care to protect the confidentiality of electronic files and (2) where the lawyer has entrusted the files to an outside provider, (a) there must be “an enforceable obligation to preserve confidentiality and security,” and (b) “available technology to guard against reasonably foreseeable attempts to infiltrate the data” must be used.

**Maine Ethics Opinion 194 (June 20, 2008)**

Maine Ethics Opinion 194 provided guidance to an attorney who wished to use a third-party vendor to process and store electronic data of a law firm, including transcriptions of voice recordings and

---


backup of the firm’s computer files. “More specifically, the question is whether the use of such services and resources, which may involve disclosure of client information to technicians who maintain the relevant computer hardware and non-lawyer transcribers outside the sphere of the attorney’s direct control and supervision, would violate the lawyer’s obligation to maintain client confidentiality. The attorney further seeks guidance on what, if any, safeguards would make such practices permissible.”

Focusing on Maine’s equivalent to Model Rule 1.6, the Committee concluded that, “with appropriate safeguards, an attorney may utilize transcription and computer server backup services remote from both the lawyer’s physical office and the lawyer’s direct control or supervision without violating the attorney’s ethical obligation to maintain client confidentiality.” The Committee was reluctant to outline acceptable safeguards because technology can change quickly. Instead it provided that at “a minimum, the lawyer should take steps to ensure that the company providing transcription or confidential data storage has a legally enforceable obligation to maintain the confidentiality of the client data involved.”

**Nevada Bar Ethics Opinion No. 33 (Feb. 9, 2006)**

The situation posed by the inquiring Nevada lawyer that produced Formal Opinion No. 33 by the Standing Committee on Ethics and Professional Responsibility of the Nevada Bar was the storage of electronic client files on a server physically located and maintained by a third party outside of the attorney’s direct supervision and control. The Committee assumed that the attorney could by contract require “all reasonable necessary means” to preserve confidentiality and prevent unauthorized access. It also assumed, however, that employees of the third party would have access, “both authorized and unauthorized” to the client confidential information. The question presented was whether the attorney violated Nevada SCR 156 (Nevada’s version of Model Rule 1.6) by storing the information in this manner without client consent.

Relying heavily on ABA Formal Ethics Opinions interpreting Model Rule 1.6, the Committee determined that the lawyer’s proposed storage plan was ethically permissible as long as the lawyer acted “reasonably and competently to protect the information from inadvertent and unauthorized access and disclosure.”

---

44 The Committee cited ABA Ethics Opinion 95-398 for the proposition that a “lawyer who allows computer maintenance company access to lawyer’s files must ensure that company establishes reasonable procedures to protect confidentiality of information in files, and would be ‘well-advised to secure company’s written assurance of confidentiality’” and N.J. Sup. Comm. Prof. Ethics Opinion 701 for the proposition that “Lawyers may maintain client files electronically with a third party as long as the third party has an enforceable obligation to preserve the security of those files and uses technology to guard against reasonably foreseeable hacking.”

45 [http://nvbar.org/sites/default/files/opinion_33.pdf](http://nvbar.org/sites/default/files/opinion_33.pdf)

46 The Committee said the attorney must; (1) exercise reasonable care in the selection of the third party contractor, “such that the contractor can be reasonably relied upon to keep the information confidential”; have “a reasonable expectation that the information will be kept confidential”; and instruct and require the third party contractor “to keep the information confidential and inaccessible.”
CONCLUSION
The message of these ethics opinions is clear: lawyers and law firms can engage third-party vendors in the cloud to store confidential information but they must do so competently with adequate supervision and implement reasonable steps to protect the confidentiality of the data. When one does business in the cloud, not every threat to confidentiality may be visible. Hence, lawyers must also stay abreast of changes in technology. As the ethics opinions discussed in this paper demonstrate, there are a number of security, data access, and data ownership and transfer issues that must be confronted by lawyers who wish to use cloud-computing services for data access and storage. Prudent lawyers will evaluate their current vulnerability to breaches of data security and the risk of data loss. They will then proceed cautiously and with expert help before they move away from existing forms of electronic data storage that do not present the array of cloud computing concerns outlined by the ABA 20/20 Commission or the Pennsylvania State Bar Ethics Committee.
ABOUT THE AUTHOR

John M. Barkett

Mr. Barkett is a partner at the law firm of Shook, Hardy & Bacon L.L.P. in its Miami office. He is a graduate of the University of Notre Dame (B.A. Government, 1972, *summa cum laude*) and the Yale Law School (J.D. 1975) and served as a law clerk to the Honorable David W. Dyer on the old Fifth Circuit Court of Appeals. Mr. Barkett is an adjunct professor of law at the University of Miami School of Law.

Mr. Barkett has, over the years, been a commercial litigator (contract and corporate disputes, employment, trademark, and antitrust), environmental litigator (CERCLA, RCRA, and toxic tort), and, for the past several years, a peacemaker and problem solver, serving as an arbitrator, mediator, facilitator, or allocator in a variety of environmental, commercial, or reinsurance contexts. He is a certified mediator under the rules of the Supreme Court of Florida and the Southern and Middle Districts of Florida and a member of the LCIA, and serves on the AAA and ICDR roster of neutrals, the CPR Institute for Dispute Resolution’s “Panel of Distinguished Neutrals,” and the National Roster of Environmental Dispute Resolution and Consensus Building Professionals maintained by the U.S. Institute for Environmental Conflict Resolution. He has served or is serving as a neutral in scores of matters involving in the aggregate more than $4 billion. He has conducted or is conducting commercial domestic and international arbitrations under AAA, LCIA, ICDR, UNCITRAL, and CPR rules and has conducted *ad hoc* arbitrations. In November 2003, he was appointed by the presiding judge to serve as the Special Master to oversee the implementation and enforcement of the 1992 Consent Decree between the United States and the State of Florida relating to the restoration of the Florida Everglades. He also consults with major corporations on the evaluation of legal strategy and risk and conducts independent investigations where such services are needed.

In March 2012, the Chief Justice appointed Mr. Barkett to serve on the Advisory Committee for Civil Rules of the Federal Judicial Conference. Mr. Barkett had been serving as the ABA Section of Litigation’s liaison to the Advisory Committee since 2009. Mr. Barkett is also a former member of the Council of the ABA Section of Litigation.

Mr. Barkett has published two books, *E-Discovery: Twenty Questions and Answers*, (Chicago: First Chair Press, 2008) and *The Ethics of E-Discovery* (Chicago: First Chair Press, 2009). Mr. Barkett has also prepared analyses of the Roberts Court the past five years, in addition to a number of other articles on a variety of topics:

Lawyer-Client Fallout: Using Privileged Information To Establish A Claim Against a Client/Employer (ABA Section of Litigation Annual Conference, Chicago, April 25, 2013)

Chess Anyone? Selection of International Commercial Arbitration Tribunals, (Miami-Dade County Bench and Bar Conference, February 8, 2013)

The Roberts Court 2011-12: The Affordable Care Act and More (ABA Annual Meeting, Chicago, August 3, 2012)


E-Communications: Problems Posed by Privilege, Privacy, and Production (ABA National Institute on E-Discovery, New York, NY, May 18, 2012)

The 7th Circuit Pilot Project: What We Might Learn And Why It Matters to Every Litigant in America (ABA Section of Litigation News Online, December 11, 2011) http://apps.americanbar.org/litigation/litigationnews/civil_procedure/docs/barkett.december11.pdf


The Challenge of Electronic Communication, Privilege, Privacy, and Other Myths, 38 Litigation Journal 17 (ABA Section of Litigation, Fall 2011)


The Roberts Court 2010-11: Three Women Justices! (ABA Annual Meeting, Toronto, August 2011)

The Ethics of Web 2.0, (ACEDS Conference, Hollywood, FL March 2011)

The Roberts Court: Year Four, Welcome Justice Sotomayor (ABA Annual Meeting, San Francisco, August 2010)

The Myth of Culture Clash in International Commercial Arbitration (co-authored with Jan Paulsson), 5 Florida International University Law Review 1 (June 2010)


From Canons to Cannon in A Century of Legal Ethics: Trial Lawyers and the ABA Canons of Professional Ethics (American Bar Association, Chicago, 2009)

The Robert’s Court: Three’s a Charm (ABA Annual Meeting, Chicago, August 2009)

Cheap Talk? Witness Payments and Conferring with Testify Witnesses, (ABA Annual Meeting, Chicago, 2009)

Burlington Northern: The Super Quake and Its Aftershocks, 58 Chemical Waste Lit. Rprt. 5 (June 2009)
Fool’s Gold: The Mining of Metadata (ABA’s Third Annual National Institute on E-Discovery, Chicago, May 22, 2009)

More on the Ethics of E-Discovery (ABA’s Third Annual National Institute on E-Discovery, Chicago, May 22, 2009)

Production of Electronically Stored Information in Arbitration: Sufficiency of the IBA Rules in Electronic Disclosure in International Arbitration (JurisNet LLC, New York, September 2008)

The Robert’s Court: The Terrible Two’s or Childhood Bliss? (ABA Annual Meeting, New York, August 2008)

Orphan Shares, 23 NRE 46 (Summer 2008)

Tipping The Scales of Justice: The Rise of ADR, 22 NRE 40 (Spring 2008)

Tattletales or Crimestoppers: Disclosure Ethics Under Model Rules 1.6 and 1.13, (ABA Annual Meeting, Atlanta, August 7, 2004 and, in an updated version, ABA Tort and Insurance Practice Section Spring CLE Meeting, Phoenix, April 11, 2008)

E-Discovery For Arbitrators, 1 Dispute Resolution International Journal 129, International Bar Association (Dec. 2007)

The Roberts Court: Where It’s Been and Where It’s Going (ABA Annual Meeting, San Francisco, August, 2007)

Help Has Arrived…Sort Of: The New E-Discovery Rules, ABA Section of Litigation Annual Meeting, San Antonio (2007)

Refresher Ethics: Conflicts of Interest, (January 2007 ABA Section of Litigation Joint Environmental, Products Liability, and Mass Torts CLE program)


The Battle For Bytes: New Rule 26, e-Discovery, Section of Litigation (February 2006)


The MJP Maze: Avoiding the Unauthorized Practice of Law (2005 ABA Section of Litigation Annual Conference)


The CERCLA Limitations Puzzle, 19 N.R.E. 70 (Fall, 2004)


Mr. Barkett is also the author of Ethical Issues in Environmental Dispute Resolution, a chapter in the ABA publication, Environmental Dispute Resolution, An Anthology of Practical Experience (July 2002) and the editor and one of the authors of the ABA Section of Litigation’s Monograph, Ex Parte Contacts with Former Employees (Environmental Litigation Committee, October 2002).

Mr. Barkett is a Fellow of the American College of Environmental Lawyers. At the University of Miami Law School, Mr. Barkett teaches two courses, “Environmental Litigation” and “E-Discovery.”

Mr. Barkett has been recognized in the areas of alternative dispute resolution or environmental law in a number of lawyer-recognition publications, including Who’s Who Legal (International Bar Association) (since 2005); Best Lawyers in America (National Law Journal) (since 2005); Legal Elite
(since 2004), (Florida Trend), Florida Super Lawyers (since 2008), and Chambers USA America’s Leading Lawyers (since 2004). Mr. Barkett can be reached at jbarkett@shb.com.